

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-222618

(43) 公開日 平成10年(1998) 8月21日

(51) Int.Cl.<sup>6</sup>  
G 0 6 K 17/00

識別記号

F I  
G 0 6 K 17/00

B

D

T

19/10

H 0 4 M 15/00

Z

19/00

17/02

A

審査請求 未請求 請求項の数28 O L (全 28 頁) 最終頁に続く

(21) 出願番号 特願平9-19399

(22) 出願日 平成9年(1997) 1月31日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 西岡 満

神奈川県川崎市幸区柳町70番地 東芝イン

テリジェントテクノロジー株式会社内

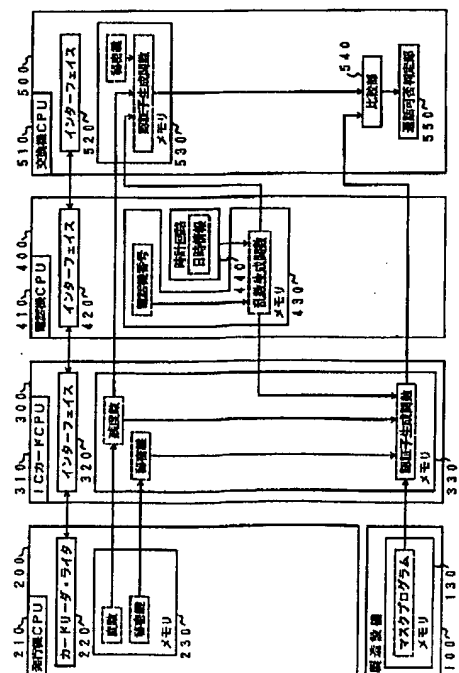
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 ICカード及びICカード処理システム

(57) 【要約】

【課題】 セキュリティの要となる秘密情報が漏洩しにくいICカード処理システムを提供すること

【解決手段】 ICカード(200)、このICカードを取り扱う端末(300)、及びこの端末を監視するホスト(400)を有するICカード処理システムにおいて、前記ICカード中で、外部への読み出しが禁止されたキーデータ及び前記端末からの端末データから第1の認証データを生成し、前記端末中で、端末固有データから乱数データを生成し、前記ホスト中で、前記キーデータ及び前記端末からの乱数データから第2の認証データを生成し、この第2の認証データと前記ICカード中で生成され前記端末を介して供給される第2の認証データとを比較してICカードの真偽を判別することを特徴とするICカード処理システム。



## 【特許請求の範囲】

【請求項1】各種演算処理を実行する集積回路を有するICカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、外部への読み出しが禁止されたキーデータを記憶する記憶手段と、前記キーデータ及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするICカード。

【請求項2】各種演算処理を実行する集積回路を有するICカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、プリペイドカードとしての価値を示す度数データを記憶する第1の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第2の記憶手段と、前記度数データ、キーデータ、及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするICカード。

【請求項3】各種演算処理を実行する集積回路を有するICカード、このICカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するICカード処理システムにおいて、前記ICカードに設けられた集積回路が、前記端末装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、外部への読み出しが禁止されたキーデータを記憶する第1の記憶手段と、この第1の記憶手段に記憶されたキーデータ、及び前記端末装置から供給される端末データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記端末装置が、前記ICカード及び前記ホスト装置との間で各種データの受け渡しを行う第2のデータ入出力手段と、この端末装置の端末固有データを記憶する第2の記憶手段と、この第2の記憶手段に記憶された端末固有データを基にして乱数データを生成する乱数データ生成手段と、を備え、前記ホスト装置が、前記端末装置との間で各種データの受け渡しを行う第3のデータ入出力手段と、

前記第1の記憶手段に記憶されたものと同じキーデータを記憶する第3の記憶手段と、

この第3の記憶手段に記憶されたキーデータ及び前記端末装置から供給される乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、

この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成された前記端末装置を介して供給される認証データとを比較する比較手段と、

この比較手段による比較結果から、前記端末装置で取り扱われるICカードの真偽を判別し、前記端末装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、

を備えたことを特徴とするICカード処理システム。

【請求項4】前記ICカードに設けられた集積回路が、プリペイドカードとしての価値を示す度数データを記憶する第4の記憶手段を備え、

前記第1の認証データ生成手段が、前記第1の記憶手段に記憶されたキーデータ、前記第4の記憶手段に記憶された度数データ、及び前記端末装置から供給される乱数データを基にして認証データを生成し、

前記第2の認証データ生成手段が、前記第3の記憶手段に記憶されたキーデータ、前記第4の記憶手段に記憶された前記端末装置を介して供給される度数データ、及び前記端末装置から供給される乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する、

ことを特徴とする請求項3に記載のICカード処理システム。

【請求項5】前記端末装置が、日時データを得るための時計を備え、

前記乱数データ生成手段が、前記第2の記憶手段に記憶された端末固有データ、及び前記時計から得られる日時データを基にして乱数データを生成する、

ことを特徴とする請求項3に記載のICカード処理システム。

【請求項6】前記ICカードの集積回路に対して前記キーデータを書き込みICカードを発行するカード発行装置を含むことを特徴とする請求項3又は請求項5に記載のICカード処理システム。

【請求項7】前記ICカードの集積回路に対して前記キーデータ及び前記度数データを書き込みICカードを発行するカード発行装置を含むことを特徴とする請求項4に記載のICカード処理システム。

【請求項8】各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するICカード、このICカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電

話機とを接続する交換機を有するICカード処理システムにおいて、  
 前記ICカードに設けられた集積回路が、  
 前記電話機との間で各種データの受け渡しを行う第1のデータ入出力手段と、  
 前記度数データを記憶する第1の記憶手段と、  
 外部への読み出しが禁止されたキーデータを記憶する第2の記憶手段と、  
 前記第1の記憶手段に記憶された度数データ、前記第2の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、  
 を備え、  
 前記電話機が、  
 前記ICカード及び前記交換機との間で各種データの受け渡しを行う第2のデータ入出力手段と、  
 電話機固有の電話機固有データを記憶する第3の記憶手段と、  
 日時データを得るための時計と、  
 前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、  
 を備え、  
 前記交換機が、  
 前記電話機との間で各種データの受け渡しを行う第3のデータ入出力手段と、  
 前記第2の記憶手段に記憶されたものと同じキーデータを記憶する第4の記憶手段と、  
 前記第1の記憶手段に記憶され前記電話機を介して供給される度数データ、前記第4の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、  
 この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、  
 この比較手段による比較結果から、前記電話機で取り扱われるICカードの真偽を判別し、前記電話機で取り扱われるICカードによる通話の可否を判定する判定手段と、  
 を備えたことを特徴とするICカード処理システム。  
 【請求項9】各種演算処理を実行する集積回路を有するICカードにおいて、  
 この集積回路が、  
 外部との間で各種データの受け渡しを行うデータ入出力手段と、  
 このICカード固有のカード固有データを記憶する第1の記憶手段と、  
 外部への読み出しが禁止されたキーデータを記憶する第

2の記憶手段と、  
 前記カード固有データ、前記キーデータ、及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、  
 を備えたことを特徴とするICカード。

【請求項10】各種演算処理を実行する集積回路を有するICカードにおいて、  
 この集積回路が、  
 外部との間で各種データの受け渡しを行うデータ入出力手段と、  
 プリペイドカードとしての価値を示す度数データを記憶する第1の記憶手段と、  
 このICカード固有のカード固有データを記憶する第2の記憶手段と、  
 外部への読み出しが禁止されたキーデータを記憶する第3の記憶手段と、  
 前記度数データ、前記カード固有データ、前記キーデータ、及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、  
 を備えたことを特徴とするICカード。

【請求項11】前記キーデータとして異なる複数のキーデータを設定し、状況に応じてこれら複数のキーデータを使い分けることを特徴とする請求項9又は10に記載のICカード。

【請求項12】各種演算処理を実行する集積回路を有するICカードを発行する発行装置、この発行装置により発行されるICカード、及びこのICカードを取り扱うカード処理装置を有するICカード処理システムにおいて、  
 前記発行装置が、  
 前記ICカードの集積回路に対して、ICカード固有のカード固有データ及びキーデータを書き込む書込手段を備え、  
 前記ICカードに設けられた集積回路が、  
 前記カード処理装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、  
 前記カード固有データを記憶する第1の記憶手段と、  
 前記キーデータを外部への読み出しを禁止した状態で記憶する第2の記憶手段と、  
 前記カード固有データ、前記キーデータ、及び前記カード処理装置から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、  
 を備え、  
 前記カード処理装置が、  
 前記ICカードとの間で各種データの受け渡しを行う第2のデータ入出力手段と、  
 このカード処理装置のカード処理装置固有データを記憶

する第3の記憶手段と、  
 この第3の記憶手段に記憶されたカード処理装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、  
 前記第2の記憶手段に記憶されたものと同じキーデータを記憶する第4の記憶手段と、  
 前記第1の記憶手段に記憶されICカードから供給されるカード固有データ、前記第4の記憶手段に記憶されたキーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、  
 この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記ICカードから供給される認証データとを比較する比較手段と、  
 この比較手段による比較結果から、前記カード処理装置で取り扱われるICカードの真偽を判別し、前記カード処理装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、  
 を備えたことを特徴とするICカード処理システム。  
 【請求項13】各種演算処理を実行する集積回路を有するICカードを発行する発行装置、この発行装置により発行されるICカード、このICカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するICカード処理システムにおいて、  
 前記発行装置が、  
 前記ICカードの集積回路に対して、ICカード固有のカード固有データ及びキーデータを書き込む書込手段を備え、  
 前記ICカードに設けられた集積回路が、  
 前記カード処理装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、  
 前記カード固有データを記憶する第1の記憶手段と、  
 前記キーデータを外部への読み出しを禁止した状態で記憶する第2の記憶手段と、  
 前記カード固有データ、前記キーデータ、及び前記端末装置から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、  
 を備え、  
 前記端末装置が、  
 前記ICカード及び前記ホスト装置との間で各種データの受け渡しを行う第2のデータ入出力手段と、  
 この端末装置の端末固有データを記憶する第3の記憶手段と、  
 この第3の記憶手段に記憶された端末固有データを基にして前記乱数データを生成する乱数データ生成手段と、  
 を備え、  
 前記ホスト装置が、

前記端末装置との間で各種データの受け渡しを行う第3のデータ入出力手段と、  
 前記第2の記憶手段に記憶されたものと同じキーデータを記憶する第4の記憶手段と、  
 前記第1の記憶手段に記憶されICカードから供給されるカード固有データ、前記第4の記憶手段に記憶されたキーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、  
 この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、  
 この比較手段による比較結果から、前記端末装置で取り扱われるICカードの真偽を判別し、前記端末装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、  
 を備えたことを特徴とするICカード処理システム。  
 【請求項14】前記ICカードに設けられた集積回路が、プリペイドカードとしての価値を示す度数データを記憶する第5の記憶手段を備え、  
 前記第1の認証データ生成手段が、前記第1の記憶手段に記憶されたカード固有データ、前記第2の記憶手段に記憶されたキーデータ、前記第5の記憶手段に記憶された度数データ、及び前記端末装置から供給される乱数データを基にして認証データを生成し、  
 前記第2の認証データ生成手段が、前記第1の記憶手段に記憶され前記端末装置を介して供給されるカード固有データ、前記第4の記憶手段に記憶されたキーデータ、前記第5の記憶手段に記憶され前記端末装置を介して供給される度数データ、及び前記端末装置から供給される乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する、  
 ことを特徴とする請求項13に記載のICカード処理システム。  
 【請求項15】前記端末装置が、日時データを得るための時計を備え、  
 前記乱数データ生成手段が、前記第3の記憶手段に記憶された端末固有データ、及び前記時計から得られる日時データを基にして乱数データを生成する、  
 ことを特徴とする請求項13に記載のICカード処理システム。  
 【請求項16】各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するICカードを発行する発行装置、この発行装置により発行されるICカード、このICカードの集積回路に記憶された度数データの度数と引き替えに通話可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するICカード

処理システムにおいて、  
 前記発行装置が、  
 前記ＩＣカードの集積回路に対して、ＩＣカード固有のカード固有データ、度数データ、及びキーデータを書き込む書込手段を備え、  
 前記ＩＣカードに設けられた集積回路が、  
 前記電話機との間で各種データの受け渡しを行う第１のデータ入出力手段と、  
 前記カード固有データを記憶する第１の記憶手段と、  
 前記度数データを記憶する第２の記憶手段と、  
 前記キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、  
 前記第１の記憶手段に記憶されたカード固有データ、前記第２の記憶手段に記憶された度数データ、前記第３の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、  
 を備え、  
 前記電話機が、  
 前記ＩＣカード及び前記交換機との間で各種データの受け渡しを行う第２のデータ入出力手段と、  
 電話機固有の電話機固有データを記憶する第４の記憶手段と、  
 日時データを得るための時計と、  
 前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、  
 を備え、  
 前記交換機が、  
 前記電話機との間で各種データの受け渡しを行う第３のデータ入出力手段と、  
 前記第３の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、  
 前記第１の記憶手段に記憶され前記電話機を介して供給されるカード固有データ、前記第２の記憶手段に記憶され前記電話機を介して供給される度数データ、前記第５の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、  
 この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、  
 この比較手段による比較結果から、前記電話機で取り扱われるＩＣカードの真偽を判別し、前記電話機で取り扱われるＩＣカードによる通話の可否を判定する判定手段と、  
 を備えたことを特徴とするＩＣカード処理システム。

【請求項１７】前記キーデータとして異なる複数のキー

データを設定し、状況に応じてこれら複数のキーデータを使い分けることを特徴とする請求項１２、請求項１３、又は請求項１６に記載のＩＣカード処理システム。  
 【請求項１８】各種演算処理を実行する集積回路を有するＩＣカードにおいて、  
 この集積回路が、  
 外部との間で各種データの受け渡しを行うデータ入出力手段と、  
 このＩＣカード固有のカード固有データを記憶する第１の記憶手段と、  
 外部への読み出しが禁止されたものであって、前記カード固有データから生成されるカード固有のカード固有キーデータを記憶する第２の記憶手段と、  
 前記カード固有キーデータ及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、  
 を備えたことを特徴とするＩＣカード。  
 【請求項１９】各種演算処理を実行する集積回路を有するＩＣカードにおいて、  
 この集積回路が、  
 外部との間で各種データの受け渡しを行うデータ入出力手段と、  
 プリペイドカードとしての価値を示す度数データを記憶する第１の記憶手段と、  
 このＩＣカード固有のカード固有データを記憶する第２の記憶手段と、  
 外部への読み出しが禁止されたものであって、前記カード固有データから生成されるカード固有のカード固有キーデータを記憶する第３の記憶手段と、  
 前記度数データ、カード固有キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、  
 を備えたことを特徴とするＩＣカード。  
 【請求項２０】前記カード固有キーデータとして異なる複数のカード固有キーデータを設定し、状況に応じてこれら複数のカード固有キーデータを使い分けることを特徴とする請求項１８又は１９に記載のＩＣカード。  
 【請求項２１】各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、及びこのＩＣカードを取り扱うカード処理装置を有するＩＣカード処理システムにおいて、  
 前記発行装置が、  
 キーデータを記憶する第１の記憶手段と、  
 前記キーデータ及びＩＣカードに対して付与されるＩＣカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第１のカード固有キーデータ生成手段と、  
 前記ＩＣカードの集積回路に対して、前記カード固有デ

ータ及び前記カード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、  
 前記ICカードに設けられた集積回路が、  
 前記カード処理装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、  
 前記カード固有データを記憶する第2の記憶手段と、  
 前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第3の記憶手段と、  
 前記カード固有キーデータ及び前記カード処理装置から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、  
 を備え、  
 前記カード処理装置が、  
 前記ICカードとの間で各種データの受け渡しを行う第2のデータ入出力手段と、  
 このカード処理装置のカード処理装置固有データを記憶する第4の記憶手段と、  
 この第4の記憶手段に記憶されたカード処理装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、  
 前記第1の記憶手段に記憶されたものと同じキーデータを記憶する第5の記憶手段と、  
 この第5の記憶手段に記憶されたキーデータ、及び前記第2の記憶手段に記憶され前記ICカードを介して供給されるカード固有データに基づき、前記第1のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第2のカード固有キーデータ生成手段と、  
 前記第2のカード固有キーデータ生成手段により生成されるカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、  
 この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記ICカードから供給される認証データとを比較する比較手段と、  
 この比較手段による比較結果から、前記カード処理装置で取り扱われるICカードの真偽を判別し、前記カード処理装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、  
 を備えたことを特徴とするICカード処理システム。  
 【請求項22】各種演算処理を実行する集積回路を有するICカードを発行する発行装置、この発行装置により発行されるICカード、このICカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するICカード処理システムにおいて、  
 前記発行装置が、  
 キーデータを記憶する第1の記憶手段と、

前記キーデータ及びICカードに対して付与されるICカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第1のカード固有キーデータ生成手段と、  
 前記ICカードの集積回路に対して、前記カード固有データ及び前記第1のカード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、  
 前記ICカードに設けられた集積回路が、  
 前記端末装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、  
 前記カード固有データを記憶する第2の記憶手段と、  
 前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第3の記憶手段と、  
 前記カード固有キーデータ及び前記端末装置から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、  
 を備え、  
 前記端末装置が、  
 前記ICカードとの間で各種データの受け渡しを行う第2のデータ入出力手段と、  
 この端末装置の端末固有データを記憶する第4の記憶手段と、  
 この第4の記憶手段に記憶された端末装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、  
 前記ホスト装置が、  
 前記端末装置との間で各種データの受け渡しを行う第3のデータ入出力手段と、  
 前記第1の記憶手段に記憶されたものと同じキーデータを記憶する第5の記憶手段と、  
 この第5の記憶手段に記憶されたキーデータ、及び前記第2の記憶手段に記憶され前記ICカードを介して供給されるカード固有データに基づき、前記第1のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第2のカード固有キーデータ生成手段と、  
 前記第2のカード固有キーデータ生成手段により生成されたカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、  
 この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、  
 この比較手段による比較結果から、前記端末装置で取り扱われるICカードの真偽を判別し、前記端末装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、

を備えたことを特徴とするICカード処理システム。

【請求項23】前記ICカードに設けられた集積回路が、プリペイドカードとしての価値を示す度数データを記憶する第6の記憶手段を備え、  
前記第1の認証データ生成手段が、前記第3の記憶手段に記憶されたカード固有キーデータ、前記第6の記憶手段に記憶された度数データ、及び前記端末装置から供給される乱数データを基にして認証データを生成し、  
前記第2の認証データ生成手段が、前記第2のカード固有キーデータ生成手段により生成されるカード固有キーデータ、前記第6の記憶手段に記憶され前記端末装置を介して供給される度数データ、及び前記端末装置から供給される乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する、  
ことを特徴とする請求項22に記載のICカード処理システム。

【請求項24】前記端末装置が、日時データを得るための時計を備え、  
前記乱数データ生成手段が、前記第4の記憶手段に記憶された端末固有データ、及び前記時計から得られる日時データを基にして乱数データを生成する、  
ことを特徴とする請求項24に記載のICカード処理システム。

【請求項25】各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するICカードを発行する発行装置、この発行装置により発行されるICカード、このICカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するICカード処理システムにおいて、  
前記発行装置が、  
キーデータを記憶する第1の記憶手段と、  
前記キーデータ及びICカードに対して付与されるICカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第1のカード固有キーデータ生成手段と、  
前記ICカードの集積回路に対して、前記カード固有データ及び前記第1のカード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、  
前記ICカードに設けられた集積回路が、  
前記電話機との間で各種データの受け渡しを行う第1のデータ入出力手段と、  
前記カード固有データを記憶する第2の記憶手段と、  
前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第3の記憶手段と、  
前記カード固有キーデータ及び前記電話機から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段

と、  
を備え、  
前記電話機が、  
前記ICカードとの間で各種データの受け渡しを行う第2のデータ入出力手段と、  
この電話機の電話機固有データを記憶する第4の記憶手段と、  
日時データを得るための時計と、  
前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、  
前記交換機が、  
前記電話機との間で各種データの受け渡しを行う第3のデータ入出力手段と、  
前記第1の記憶手段に記憶されたものと同じキーデータを記憶する第5の記憶手段と、  
この第5の記憶手段に記憶されたキーデータ、及び前記第2の記憶手段に記憶され前記電話機を介して供給されるカード固有データに基づき、前記第1のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第2のカード固有キーデータ生成手段と、  
この第2のカード固有キーデータ生成手段により生成されたカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、  
この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、  
この比較手段による比較結果から、前記電話機で取り扱われるICカードの真偽を判別し、前記電話機で取り扱われるICカードによる通話の可否を判定する判定手段と、  
を備えたことを特徴とするICカード処理システム。

【請求項26】前記キーデータとして異なる複数のキーデータを設定し、状況に応じてこれら複数のキーデータを使い分けることを特徴とする請求項21、請求項22、又は請求項25に記載のICカード処理システム。

【請求項27】前記固有キーデータ生成手段として異なる複数の固有キーデータ生成手段を設定し、状況に応じてこれら複数の固有キーデータ生成手段を使い分けることを特徴とする請求項21、請求項22、又は請求項25に記載のICカード処理システム。

【請求項28】前記キーデータとして異なる複数のキーデータを設定し、かつ前記固有キーデータ生成手段として異なる複数の固有キーデータ生成手段を設定し、状況に応じてこれら複数のキーデータ及びこれら複数の固有キーデータ生成手段を使い分けることを特徴とする請求項21、請求項22、又は請求項25に記載のICカード処理システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、演算素子としてのICを有するICカードを処理をするICカード処理システムに関する。

## 【0002】

【従来の技術】現在、プリペイドカードの一種であるテレホンカードにより公衆電話が利用できるようになっている。また、将来的には、ICカードにプリペイドカードとしての機能を持たせ、このICカードにより公衆電話が利用できるよう提案がなされている。

【0003】上記したようにICカードをプリペイドカードとして使用する場合、機器（電話機）によるカードの正当性確認（真偽判定）は、例えば、機器に固定で保持されているキー情報、又はカード使用者により入力される暗証番号の「値の照合」により行われる。

【0004】また、より進んだ方法として、ICカードが持つ乱数生成機能を利用した認証方法では、全てのカードに共通な値として格納されたキーを暗号化に使用して認証が行われる。さらに、このような認証処理が行なわれる場合、カードには一種類の暗号化キーを使用した一種類の暗号処理が適用される。

【0005】以上説明した処理は基本的にカードを保持する機器内で、その機器が格納しているプログラム等により行なわれる。

## 【0006】

【発明が解決しようとする課題】ところが、上記した従来のようなカードの正当性確認の方法では、以下のような問題があった。

【0007】機器に固定で保持されているキー情報、又はカード使用者により入力される暗証番号等の「値の照合」によりカードの正当性を確認する場合、カードと機器の伝送内容を何らかの方法でモニターされてしまうことがある。この場合、モニターされたデータが、カード偽造・システム解析の手がかりとされてしまうことがある。

【0008】ICカードが持つ乱数生成機能を利用した認証方法では、カードと機器の間の通信で交換される乱数は都度異なる値となり、単純に内容をモニターするだけでは直接カード偽造・システム解析の手がかりとすることはできない。ところが、交わされる乱数の組を複数収集して解析することによりカード偽造・システム解析の手がかりが得られてしまうことがある。さらに、認証処理が行なわれる場合に使用される暗号化処理は一種類のため、交わされる乱数の組を複数収集して解析することによりカード偽造・システム解析の手がかりが得られてしまうことがある。

【0009】これらの処理は基本的にカードを保持する機器内で、その機器が格納しているプログラム等により行なわれているため、機器を入手してプログラムを解析

することによりカード偽造・システム解析の手がかりが得られてしまうことがある。

【0010】この発明の目的は、上記したような事情に鑑み成されたものであって、セキュリティの要となる秘密情報が漏洩しにくいICカード処理システムを提供することにある。さらに、セキュリティの要となる秘密情報が漏洩した場合でも、漏洩した秘密情報による不正使用を防止できるICカード処理システムを提供することにある。

## 10 【0011】

【課題を解決するための手段】この発明は、上記問題点に基づきなされたもので、この発明によれば、各種演算処理を実行する集積回路を有するICカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、外部への読み出しが禁止されたキーデータを記憶する記憶手段と、前記キーデータ及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするICカードが提供される。

20 【0012】また、この発明によれば、各種演算処理を実行する集積回路を有するICカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、プリペイドカードとしての価値を示す度数データを記憶する第1の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第2の記憶手段と、前記度数データ、キーデータ、及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするICカードが提供される。

30 【0013】さらに、この発明によれば、各種演算処理を実行する集積回路を有するICカード、このICカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するICカード処理システムにおいて、前記ICカードに設けられた集積回路が、前記端末装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、外部への読み出しが禁止されたキーデータを記憶する第1の記憶手段と、この第1の記憶手段に記憶されたキーデータ、及び前記端末装置から供給される端末データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記端末装置が、前記ICカード及び前記ホスト装置との間で各種データの受け渡しを行う第2のデータ入出力手段と、この端末装置の端末固有データを記憶する第2の記憶手段と、この第2の記憶手段に記憶された端末固有データを基にして乱数データを生成する乱数データ生成手段と、を備え、前記ホスト装置が、前記端末装置との間で各種データの受け渡しを行う第3のデータ入出力手段と、前記第1の記憶手段に記憶されたものと同一キーデータを記憶する第3の記憶手段と、この第3の



記憶手段に記憶されたキーデータ及び前記端末装置から供給される乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記端末装置で取り扱われるICカードの真偽を判別し、前記端末装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするICカード処理システムが提供される。

【0014】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するICカード、このICカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するICカード処理システムにおいて、前記ICカードに設けられた集積回路が、前記電話機との間で各種データの受け渡しを行う第1のデータ入出力手段と、前記度数データを記憶する第1の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第2の記憶手段と、前記第1の記憶手段に記憶された度数データ、前記第2の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記電話機が、前記ICカード及び前記交換機との間で各種データの受け渡しを行う第2のデータ入出力手段と、電話機固有の電話機固有データを記憶する第3の記憶手段と、日時データを取得するための時計と、前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、を備え、前記交換機が、前記電話機との間で各種データの受け渡しを行う第3のデータ入出力手段と、前記第2の記憶手段に記憶されたものと同じキーデータを記憶する第4の記憶手段と、前記第1の記憶手段に記憶され前記電話機を介して供給される度数データ、前記第4の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記電話機で取り扱われるICカードの真偽を判別し、前記電話機で取り扱われるICカードによる通話の可否を判定する判定手段と、を備えたことを特徴とするICカード処理システムが提供される。

【0015】またさらに、この発明によれば、各種演算

処理を実行する集積回路を有するICカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、このICカード固有のカード固有データを記憶する第1の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第2の記憶手段と、前記カード固有データ、前記キーデータ、及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするICカードが提供される。

【0016】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有するICカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、プリペイドカードとしての価値を示す度数データを記憶する第1の記憶手段と、このICカード固有のカード固有データを記憶する第2の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第3の記憶手段と、前記度数データ、前記カード固有データ、前記キーデータ、及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするICカードが提供される。

【0017】またさらに、この発明によれば、各種演算処理を実行する集積回路を有するICカードを発行する発行装置、この発行装置により発行されるICカード、及びこのICカードを取り扱うカード処理装置を有するICカード処理システムにおいて、前記発行装置が、前記ICカードの集積回路に対して、ICカード固有のカード固有データ及びキーデータを書き込む書込手段を備え、前記ICカードに設けられた集積回路が、前記カード処理装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、前記カード固有データを記憶する第1の記憶手段と、前記キーデータを外部への読み出しを禁止した状態で記憶する第2の記憶手段と、前記カード固有データ、前記キーデータ、及び前記カード処理装置から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記カード処理装置が、前記ICカードとの間で各種データの受け渡しを行う第2のデータ入出力手段と、このカード処理装置のカード処理装置固有データを記憶する第3の記憶手段と、この第3の記憶手段に記憶されたカード処理装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、前記第2の記憶手段に記憶されたものと同じキーデータを記憶する第4の記憶手段と、前記第1の記憶手段に記憶されICカードから供給されるカード固有データ、前記第4の記憶手段に記憶されたキーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、この第2

の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記ICカードから供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記カード処理装置で取り扱われるICカードの真偽を判別し、前記カード処理装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするICカード処理システムが提供される。

【0018】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有するICカードを発行する発行装置、この発行装置により発行されるICカード、このICカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するICカード処理システムにおいて、前記発行装置が、前記ICカードの集積回路に対して、ICカード固有のカード固有データ及びキーデータを書き込む書込手段を備え、前記ICカードに設けられた集積回路が、前記カード処理装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、前記カード固有データを記憶する第1の記憶手段と、前記キーデータを外部への読み出しを禁止した状態で記憶する第2の記憶手段と、前記カード固有データ、前記キーデータ、及び前記端末装置から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記端末装置が、前記ICカード及び前記ホスト装置との間で各種データの受け渡しを行う第2のデータ入出力手段と、この端末装置の端末固有データを記憶する第3の記憶手段と、この第3の記憶手段に記憶された端末固有データを基にして前記乱数データを生成する乱数データ生成手段と、を備え、前記ホスト装置が、前記端末装置との間で各種データの受け渡しを行う第3のデータ入出力手段と、前記第2の記憶手段に記憶されたものと同じキーデータを記憶する第4の記憶手段と、前記第1の記憶手段に記憶されICカードから供給されるカード固有データ、前記第4の記憶手段に記憶されたキーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記端末装置で取り扱われるICカードの真偽を判別し、前記端末装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするICカード処理システムが提供される。

【0019】またさらに、この発明によれば、各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するICカードを発行する発行装置、この発行装置により発行

されるICカード、このICカードの集積回路に記憶された度数データの度数と引き替えに通話可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するICカード処理システムにおいて、前記発行装置が、前記ICカードの集積回路に対して、ICカード固有のカード固有データ、度数データ、及びキーデータを書き込む書込手段を備え、前記ICカードに設けられた集積回路が、前記電話機との間で各種データの受け渡しを行う第1のデータ入出力手段と、前記カード固有データを記憶する第1の記憶手段と、前記度数データを記憶する第2の記憶手段と、前記キーデータを外部への読み出しを禁止した状態で記憶する第3の記憶手段と、前記第1の記憶手段に記憶されたカード固有データ、前記第2の記憶手段に記憶された度数データ、前記第3の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記電話機が、前記ICカード及び前記交換機との間で各種データの受け渡しを行う第2のデータ入出力手段と、電話機固有の電話機固有データを記憶する第4の記憶手段と、日時データを取得するための時計と、前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、を備え、前記交換機が、前記電話機との間で各種データの受け渡しを行う第3のデータ入出力手段と、前記第3の記憶手段に記憶されたものと同じキーデータを記憶する第5の記憶手段と、前記第1の記憶手段に記憶され前記電話機を介して供給されるカード固有データ、前記第2の記憶手段に記憶され前記電話機を介して供給される度数データ、前記第5の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記電話機で取り扱われるICカードの真偽を判別し、前記電話機で取り扱われるICカードによる通話の可否を判定する判定手段と、を備えたことを特徴とするICカード処理システムが提供される。

【0020】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有するICカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、このICカード固有のカード固有データを記憶する第1の記憶手段と、外部への読み出しが禁止されたものであって、前記カード固有データから生成されるカード固有のカード固有キーデータを記憶する第2の記憶手段と、前記カード固有キーデータ及び外部から供給される外部データを基にして、このIC

カードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするICカードが提供される。

【0021】またさらに、この発明によれば、各種演算処理を実行する集積回路を有するICカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、プリペイドカードとしての価値を示す度数データを記憶する第1の記憶手段と、このICカード固有のカード固有データを記憶する第2の記憶手段と、外部への読み出しが禁止されたものであって、前記カード固有データから生成されるカード固有のカード固有キーデータを記憶する第3の記憶手段と、前記度数データ、カード固有キーデータ、及び外部から供給される外部データを基にして、このICカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするICカードが提供される。

【0022】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有するICカードを発行する発行装置、この発行装置により発行されるICカード、及びこのICカードを取り扱うカード処理装置を有するICカード処理システムにおいて、前記発行装置が、キーデータを記憶する第1の記憶手段と、前記キーデータ及びICカードに対して付与されるICカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第1のカード固有キーデータ生成手段と、前記ICカードの集積回路に対して、前記カード固有データ及び前記カード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、前記ICカードに設けられた集積回路が、前記カード処理装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、前記カード固有データを記憶する第2の記憶手段と、前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第3の記憶手段と、前記カード固有キーデータ及び前記カード処理装置から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記カード処理装置が、前記ICカードとの間で各種データの受け渡しを行う第2のデータ入出力手段と、このカード処理装置のカード処理装置固有データを記憶する第4の記憶手段と、この第4の記憶手段に記憶されたカード処理装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、前記第1の記憶手段に記憶されたものと同じキーデータを記憶する第5の記憶手段と、この第5の記憶手段に記憶されたキーデータ、及び前記第2の記憶手段に記憶された前記ICカードを介して供給されるカード固有データに基づき、前記第1のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第2のカード固有キーデータ生成手段と、前記第2のカード固有キ

ーデータ生成手段により生成されるカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生成する第2の認証データ生成手段と、この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成された前記ICカードから供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記カード処理装置で取り扱われるICカードの真偽を判別し、前記カード処理装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするICカード処理システムが提供される。

【0023】またさらに、この発明によれば、各種演算処理を実行する集積回路を有するICカードを発行する発行装置、この発行装置により発行されるICカード、このICカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するICカード処理システムにおいて、前記発行装置が、キーデータを記憶する第1の記憶手段と、前記キーデータ及びICカードに対して付与されるICカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第1のカード固有キーデータ生成手段と、前記ICカードの集積回路に対して、前記カード固有データ及び前記第1のカード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、前記ICカードに設けられた集積回路が、前記端末装置との間で各種データの受け渡しを行う第1のデータ入出力手段と、前記カード固有データを記憶する第2の記憶手段と、前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第3の記憶手段と、前記カード固有キーデータ及び前記端末装置から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記端末装置が、前記ICカードとの間で各種データの受け渡しを行う第2のデータ入出力手段と、この端末装置の端末固有データを記憶する第4の記憶手段と、この第4の記憶手段に記憶された端末装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、前記ホスト装置が、前記端末装置との間で各種データの受け渡しを行う第3のデータ入出力手段と、前記第1の記憶手段に記憶されたものと同じキーデータを記憶する第5の記憶手段と、この第5の記憶手段に記憶されたキーデータ、及び前記第2の記憶手段に記憶された前記ICカードを介して供給されるカード固有データに基づき、前記第1のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第2のカード固有キーデータ生成手段により生成されたカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証デ

ータを生成する第2の認証データ生成手段と、この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記端末装置で取り扱われるICカードの真偽を判別し、前記端末装置で取り扱われるICカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするICカード処理システムが提供される。

【0024】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するICカードを発行する発行装置、この発行装置により発行されるICカード、このICカードの集積回路に記憶された度数データの度数と引き替えに通話可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するICカード処理システムにおいて、前記発行装置が、キーデータを記憶する第1の記憶手段と、前記キーデータ及びICカードに対して付与されるICカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第1のカード固有キーデータ生成手段と、前記ICカードの集積回路に対して、前記カード固有データ及び前記第1のカード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、前記ICカードに設けられた集積回路が、前記電話機との間で各種データの受け渡しを行う第1のデータ入出力手段と、前記カード固有データを記憶する第2の記憶手段と、前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第3の記憶手段と、前記カード固有キーデータ及び前記電話機から供給される乱数データを基にして、このICカードを認証するための認証データを生成する第1の認証データ生成手段と、を備え、前記電話機が、前記ICカードとの間で各種データの受け渡しを行う第2のデータ入出力手段と、この電話機の電話機固有データを記憶する第4の記憶手段と、日時データを得るための時計と、前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、前記交換機が、前記電話機との間で各種データの受け渡しを行う第3のデータ入出力手段と、前記第1の記憶手段に記憶されたものと同じキーデータを記憶する第5の記憶手段と、この第5の記憶手段に記憶されたキーデータ、及び前記第2の記憶手段に記憶され前記電話機を介して供給されるカード固有データに基づき、前記第1のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第2のカード固有キーデータ生成手段と、この第2のカード固有キーデータ生成手段により生成されたカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第1の認証データ生成手段と同様にして認証データを生

成する第2の認証データ生成手段と、この第2の認証データ生成手段で生成された認証データと、前記第1の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記電話機で取り扱われるICカードの真偽を判別し、前記電話機で取り扱われるICカードによる通話の可否を判定する判定手段と、を備えたことを特徴とするICカード処理システムが提供される。

【0025】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。

【0026】図1～図12は、この発明の一形態に係るICカード処理システムを構成するICカード、ICカード発行機、ICカードを直接取り扱う端末装置としての電話機、及び電話機と電話機とを取り繋ぐ交換機を説明するための図である。なお、この実施の形態では、プリペイドカードとしての価値を示す度数データをICカードに記録して、このICカードに記録された度数と引き替えに電話機が利用できるような公衆電話のシステムに適用した場合について説明する。

【0027】まず、図1を参照して、ICカードについて簡単に説明する。図1は、ICカードの外観を示す概略図である。この発明のICカード処理システムで使用されるICカード300には、図1に示すように、磁気ストライプ302及びICモジュール304などが設けられている。また、このICカード300は、ISO等の規格に基づき形成されるものとする。

【0028】ここで、ICモジュール304について簡単に説明しておく。ICモジュール304には、例えばP1～P8の8本の端子（ピン）が設けられている。P1は、後述するカードリーダー・ライタからの動作電流をカードに供給する端子である。P2は、カードリーダー・ライタからのリセット信号をカードに供給するピンである。P3は、カードリーダー・ライタからの動作クロックを供給する端子である。P5は、グランド端子である。P7は、カードリーダー・ライタからの書込電圧を供給する端子である。P8は、双方向のシリアルなデータ伝送路として機能する端子である。

【0029】続いて、図2を参照して、ICカード300の製造手順について説明する。図2は、ICカードの製造手順を示すフローチャートである。

【0030】ICカード300のICモジュール304の原型であるICチップ305は、図3に示すように、演算素子としてのCPU310、及びROM331並びにRAM332を含むメモリ330等で構成されている。このメモリ330には、CPU310を制御するカード制御プログラムが記憶される。

【0031】ICカード製造行程の始めの段階では、後述する認証子を生成するための認証子生成関数を含む前

記カード制御プログラム（マスクプログラム）が作成される（ST2）。このカード制御プログラムは、ICチップ305のメモリ330にに登録される（ST4）。カード制御プログラムが登録されたICチップ305はモジュール化され（ST6）、モジュール化されたICモジュール304はICカード300に埋め込まれる（ST8）。このようにしてICカードが製造される。

【0032】続いて、図4を参照して、ICカードを発行する発行機200について説明する。図4は、発行機200の外観を示す概略図である。

【0033】図4に示すように、発行機200は、ICカードに対してデータを書き込んだりICカードに書き込まれたデータを読み出したりするICカードリーダー・ライタ220、及びこのカードリーダー・ライタ220を制御するパーソナルコンピュータ（PC）201等により構成されている。

【0034】なお、以下説明する発行機200の機能は、このPC201を制御する発行機CPU210の制御プログラムにより実現されるものとする。勿論、これは最低限の構成であり、ICカードを多数枚発行する必要がある場合には、自動的にICカードを取り込み/送り出して複数枚を連続して自動発行する仕様が必要となる。

【0035】続いて、図5を参照して、発行機200によるICカードの発行の流れについて説明する。図5は、発行機200によるICカードの発行を説明するフローチャートである。

【0036】まず、PC201上でのデータの入力編集作業として後述する認証子を生成するための認証子生成用秘密鍵が設定される（ST11）。認証子生成用秘密鍵は、例えば、PC201のキーボードから入力したり、認証子生成用秘密鍵が記録されたディスクから読み取ったりして設定される。また、システムとして認証子生成用秘密鍵が使用される場合には、予めPC201の発行機CPU230の制御プログラムコードに含ませるようにしてもよい。あるいは、このとき使用されていないカードリーダー・ライタ220を使用して、システムとして用意された設定用ICカードから読みとるようにしてもよい。

【0037】次に、PC201の操作により、これから発行するICカードへ設定するための度数（50度数、100度数等）が選択される（ST12）。多数枚のICカードを連続発行する場合、度数ごとに複数組の発行機200を用意し各発行機ごとに扱う度数を固定するようにしてもよい。

【0038】上記したように認証子生成用秘密鍵が設定され度数が選択されるとカード発行準備が整い、カードリーダー・ライタ220でICカード挿入待ちとなる。カードリーダー・ライタ220にICカードが挿入されると（ST13）、ICカードに対して前記設定された認証

子生成用秘密鍵及び前記選択された度数が書き込まれる（ST14）。多数枚のICカードを連続発行する場合、未発行カードをまとめてスタックしておき自動的に一枚抜き取って書き込み位置まで搬送するような自動取り込み方式をとるようにしてもよい。

【0039】その後、カードリーダー・ライタ220からICカードが抜き取られ（ST15）、一枚のICカードの発行操作が完了する。多数枚のICカードを連続発行する機器の場合、発行済みICカードを自動的に搬送して機器外へ送り出したり、機器内外の発行済みICカード収納部へ搬送して積み重ねる形で格納するような自動搬送方式をとるようにしてもよい。ST13～ST15の繰り返しにより、次々とICカードが発行されることになる（ST16）。

【0040】ここで、図6～図8を参照して、設定用ICカードについて説明する。設定用ICカードとは、上記したようにICカード処理システムにおいて必要とされるデータ、例えば認証子生成用秘密鍵のようなものをシステムに設定するために使用されるものである。このような設定用ICカードを利用することにより、機密データを安全にシステムに設定することができる。勿論、この設定用ICカードに記録されているデータは容易に外部に読み出せないようになっている。

【0041】ここで、設定用ICカードから認証子生成用秘密鍵を発行機200に設定するケースについて説明する。設定用ICカードから認証子生成用秘密鍵を読み出すにあたっては、PC201即ち発行機200と設定用ICカードとの間で何らかの正当性確認をする運用が必要となる。

【0042】単純には、発行機200側のプログラムの一部として格納されているキー情報をカードへ送り、カード内で照合してキー情報の正当性が確認されてから認証子生成用秘密鍵を読み出すことができる様にする（図6）。これにより、タイプミス等による誤った値の認証子生成用秘密鍵の登録が回避されるだけでなく、認証子生成用秘密鍵はICカード300と発行機200の間の通信データとして出現するだけとなり、外部への漏洩の機会が減少する。

【0043】また、認証子生成用秘密鍵の暗号化については、設定用ICカードに暗号化機能を持たせ、生データとして記憶している認証子生成用秘密鍵を送出時に暗号化する方法（図7）や、設定用ICカードへ既に暗号化済みの認証子生成用秘密鍵を記憶させておきそのまま送出させる方法（図8）等が考えられる。

【0044】また、この様な設定用ICカードを作成する機能を、発行機200に併せ持たせる方法と、別システムとして用意する方法とが考えられる。さらに、発行機200と設定用ICカードの間の正当性確認に相互認証を使用することによって、発行機200側として偽の設定用ICカードにより偽の認証子生成用秘密鍵を設定

されることによる業務妨害が回避できる。これは、第三者が悪意で設定用ICカードをすり替えることによって、誤った認証子生成用秘密鍵が設定された正常に使用できないカードを市中に出回らせ、カード及びシステムの信頼性を失墜させる様な妨害に利用される。すなわち、システム全体の解析により電話がかけられるカードを偽造することは困難だが、設定用ICカードに相互認証を適用していなければ、発行機200からのキー照合に際していかなるキー値に対しても正当であると応え、偽の認証子生成用秘密鍵を送出する為の設定用ICカードは、幾分偽造しやすいためである。

【0045】ここで、図9を参照して上記した相互認証の手順について説明する。図9は、相互認証を説明する図である。ここでは、上位機器XとICカードYとの相互認証を例にとり説明する。

【0046】第1に、内部認証（上位機器X側での認証処理）について説明する。まず、上位機器X側で、乱数R1が生成される（ST20）。この生成された乱数R1がICカードYへ送られる（ST22）。ICカードY側において、乱数R1が予め設定された内部認証用キーK1により暗号化され、暗号化キーR2Yが生成される（ST24）。この生成された暗号化キーR2Yは、ICカードY側から上位機器X側へ送信される（ST26）。

【0047】一方、上位機器X側では、乱数R1が予め設定された内部認証用キーK1により暗号化され、暗号化キーR2Xが生成される（ST28）。この生成された暗号化キーR2Xと、ICカードY側で生成され送られてきた暗号化キーR2Yとが比較され（ST30）、この比較結果により上位機器X側において、ICカードYの真偽が判定される（ST32）。即ち、暗号化キーR2X=R2Yとなれば、ICカードYは真と判定される（以上内部認証）。

【0048】第2に、外部認証（ICカードY側での認証処理）について説明する。まず、上位機器X側からICカードYに対して、外部認証の要求が出される（ST34）。この要求に従い、ICカードY側において、乱数R3が生成される（ST36）。この生成された乱数R3が、上位機器Xへ送られる（ST38）。上位機器X側において、乱数R3が予め設定された外部認証用キーK2により暗号化され、暗号化キーR4Xが生成される（ST40）。この生成された暗号化キーR4Xは、上位機器X側からICカードY側へ送信される（ST42）。

【0049】一方、ICカードY側では、乱数R3が予め設定された内部認証用キーK2により暗号化され、暗号化キーR4Yが生成される（ST44）。この生成された暗号化キーR4Yと、上位機器X側で生成され送られてきた暗号化キーR4Xとが比較され（ST46）、この比較結果によりICカードY側において、上位機器

Xの真偽が判定される（ST48）。即ち、暗号化キーR4X=R4Yとなれば、上位機器Xは真と判定される（以上内部認証）。上位機器Xが真と判定されると、このICカードYからのデータの読み出しが許可され、比較結果がレスポンスとして上位機器Xに送信される（ST50）。

【0050】続いて、図10を参照して、電話機400について説明する。図10は、電話機400の外観を示す概略図である。

【0051】図10に示すように、電話機400は、送受話器401、プッシュ式ボタン402、ICカード300の挿入を受け付けるとともにICカード300を返却するカード挿入口403、及びICカード300に記録された度数データの残りを表示する表示部404などで構成されている。

【0052】ここで、図11を参照して、電話機400の製造手順について説明する。図11は、電話機400の製造手順を示すフローチャートである。

【0053】考え方はICカード300の製造の場合と似ており、基本的な構成のハードウェア及びこのハードを制御するソフトウェアに対して、この実施形態で適用する特別な機能を実現するためのハードとソフトを追加する事になる。

【0054】まず、ハードウェア製造時において、後述する乱数生成時における乱数生成の種の一つとなる日時データを取得するための時計回路が搭載される（ST60）。

【0055】次に、認証子を生成するために必要な乱数を生成する乱数生成プログラム、カードのアクセスプログラム、及び交換機500との間で種々のやりとりをするプログラムを、基本的な電話機制御を司る電話機制御プログラムに包含して作成する（ST62）。

【0056】このようにして作成された電話機制御プログラムを、先にハードウェアだけ製造済みの電話機400に搭載する。この方法としては、例えば別工程でこの電話機制御プログラムが書き込まれたROMを、電話機400の制御基板上のROMソケットに差し込むことで行なったり、制御基板上にあるいは機体内のメモリカード等の不揮発性あるいはバッテリーバックアップされたメモリに通信等で書き込むことで行なったり、あるいは電話機400にディスク装置を内蔵する様な場合にはこれに書き込むことで行なったりしてもよい（ST64）。

【0057】さらに、後述する乱数生成時に乱数生成のもう一つの種となる各電話機毎に固有の電話機番号（機体個別番号）を電話機に登録する必要がある。この実施形態では、前記の様な方法でプログラム登録が完了した電話機400のボタン402により電話機番号を入力し登録する（ST66）。

【0058】ここで、電話機番号の登録の一例について簡単に説明する。前記したように制御プログラムの登録

が完了した電話機400に対してはじめて電源が投入されると、電話機番号が登録されていないので電話機番号が入力されるのを待つ状態となる。すなわち、電話機のプログラムは起動の都度電話機番号の登録状態を検査し登録されていない場合、電話機番号入力待ち状態となる。このとき、カード残度数表示部404には、「――」が表示されるので、ボタン402から電話機番号が入力されることになる。まず、最初に押下されたボタン402に対応した数字が表示部404の右側に表示され、「――A」（Aは押下されたボタンに対応した数字）となる。さらに、ボタン402が押下されると「――AB」（Bは次に押下されたボタンに対応した数字）、またさらに、ボタン402が押下されると「ABC」（Cはまた次に押下されたボタンに対応した数字）、さらにまた、ボタン402が押下されると「BCD」（Dはそのまた次に押下されたボタンに対応した数字）という様に順送り表示される。最終桁までの入力が完了したら「\*」を押すと表示が点滅して確認待ちとなり「#」を押すことで入力された電話機番号が決定され電話機内部のROMに書き込まれる。一旦電話機番号が登録された後は、カード式電話機としての標準的動作に移る。

【0059】一旦電源が断たれ、再度通電して再起動した際に電話機のプログラムは電話機番号の登録状態を検査し、それが登録済みであることを確認して電話機番号登録動作をスキップしてカード式電話機としての標準的動作に移る。

【0060】上記したようにボタン402と表示部404を使う方法の他、送受話器401で音声入力したり、通信で登録したり、前記プログラム登録時にプログラムの一部として登録する等のようにしてもよい。

【0061】このような工程を経て完成した電話機400は公衆電話として市中の各所に設置されることになる。

【0062】続いて、図12参照して交換機500について説明する。図12は、交換機500の外観を示す概略図である。

【0063】図12に示すように、交換機500は、交換機本体501、及びこの交換機本体501に対して各種指示を行うパーソナルコンピュータ(PC)502などで構成されている。

【0064】ここで、図13を参照して、交換機500の製造手順について説明する。図13は、交換機500の製造手順を示すフローチャートである。

【0065】考え方は電話機400と同様であり、基本的な構成のハードウェアとそれを制御するソフトウェアに対してこの実施形態で適用する特別な機能を実現するためのハードとソフトを追加する事になる。

【0066】まずハードウェア製造時において、電話機400と通信を行うインターフェイスが搭載される(ST70)。

【0067】次に、ICカード300に登録されるのと

同じ認証子生成用秘密鍵、同じ認証子生成関数、及び電話機とICカード300との間で種々のやりとりをするプログラムを、基本的な交換機制御を司る交換機制御プログラムに包含して作成する(ST72)。

【0068】このようにして作成された交換機制御プログラムを、先にハードウェアだけ製造済みの交換機本体501に搭載する。この方法としては、例えば別工程でこの交換機制御プログラムが書き込まれたROMを、交換機の制御基板上のROMソケットに差し込むことで行なったり、制御基板上にあるいは機体内のメモリカード等の不揮発性あるいはバッテリバックアップされたメモリに通信等で書き込むことで行なったり、あるいは交換機本体501にディスク装置を内蔵する様な場合にはこれに書き込むことで行なったりしてもよい(ST74)。

【0069】このような工程を経て完成した交換機500はしかるべき管理者以外は触れられないセキュリティの確保された環境に設置される。

【0070】なお、ICカード300に格納される認証子生成用秘密鍵、プリペイドの度数、認証子生成関数のプログラムの各情報の格納タイミングの上記以外のバリエーションに限定されるものではない。例えば、認証子生成関数のプログラムだけでなく、販売額に当たる基本度数をICカードの基本プログラム(OS)の一部として製造時に登録しておき、それ以外のデータ部分について発行機で書き込むパターン(この場合の残度数は当初の基本度数をもとに計算する)や、完全なユニーク性を確保するためにはカード個別番号だけをOS内に固定データとして製造時に登録し、それ以外を発行機で書き込むパターン等が考えられる。これ以外にも種々のパターンがあるので、全ての組み合わせについてそれ以降の本発明で示す処理に適用できるため、ここに示した以外の格納タイミングのパターンを排除するものではない。

【0071】次に、この発明のポイントであるICカード処理システムにおけるセキュリティについて第1の実施形態～第3の実施形態に分けて説明する。

【0072】最初に、図14を参照して第1の実施形態について説明する。図14は、この発明の第1の実施形態に係るICカード処理システムを示す図である。

【0073】まず、製造設備100によりICカード300が製造される。このICカード製造行程では、認証子生成関数を含むマスクプログラムが作成され、この認証子生成関数を含むマスクプログラムがICチップ305のメモリ330に登録される。さらにこのICチップ305がモジュール化され、このモジュール化されたICモジュール304が、ICカードへ埋め込まれICカード300が製造される。つまり、このICカード製造行程において、ICカード300のメモリ330に対して認証子生成関数が登録されたことになる。

【0074】次に、上記のような製造行程を経て製造さ

れたICカード300に対して、発行機20による発行処理がなされる。この発行機200は、発行機CPU210により制御されており、この発行機CPU210を制御する発行機制御プログラム及びICカードに渡す度数情報等はメモリ230に記憶されている。また、この実施形態では、発行機制御プログラムに、認証子生成用秘密鍵が含まれているものとする。このような発行機200のカードリーダー・ライタ220により、ICカード300に対して度数情報及び認証子生成用秘密鍵が登録される。

【0075】次に、上記製造工程及び発行処理を経たICカード300について説明する。このICカード300は、ICカードCPU310により制御されており、このICカードCPU310を制御するカード制御プログラム及び発行機200から送られる度数情報並びに認証子生成用秘密鍵等はメモリ330に記憶されている。また、この時点で、カード制御プログラムには、認証子生成関数が含まれている。さらに、このICカード300は、電話機400との間で各種データの受け渡しを行うインターフェース320を備えている。

【0076】次に、ICカード300を取り扱う端末装置としての電話機400について説明する。この電話機400は、前記説明したような製造行程を経て製造される。つまり、電話機400は、電話機CPU410により制御されており、この電話機CPU410を制御する電話機制御プログラム及び前記した電話機番号等はメモリ430に記憶されている。また、この実施形態では、電話機制御プログラムに、乱数生成関数が含まれているものとする。さらに、この電話機400には、時計回路440が搭載され、この時計回路440から日時情報が取得される。そして、この時計回路440から得られる日時情報及びメモリ430に記憶されている電話機番号を基にして、メモリ430に記憶された電話機制御プログラムに含まれる乱数生成関数により乱数が生成される。さらに、この電話機400は、交換機500との間で各種データの受け渡しを行うインターフェース420を備えている。

【0077】次に、電話機と電話機とを接続する交換機500について説明する。交換機500は、前記説明したような製造行程を経て製造される。つまり、交換機500は、交換機CPU510により制御されており、この交換機CPU510を制御する制御プログラム及びICカード300のメモリ330に記憶された認証子生成用秘密鍵と同じ認証子生成用秘密鍵等はメモリ530に記憶されている。また、この実施形態では、交換機制御プログラムに、カード制御プログラムに含まれた認証子生成関数と同じ認証子生成関数等が含まれているものとする。さらに、この交換機500には、メモリ530内の認証子生成関数により生成された認証子と、ICカード300のメモリ330内の認証子生成関数により生成

された認証子とを比較する比較部540、及びこの比較部540の比較結果からICカード300による通話の可否を判定する判定部550を備えている。さらに、この交換機500は、電話機400との間で各種データの受け渡しを行うインターフェース520を備えている。

【0078】上記説明したような発行機200、ICカード300、電話機400、及び交換機500を有するICカード処理システムにおけるセキュリティは次のようにして守られる。

10 【0079】例えば、電話機400にICカード300が差し込まれると、電話機400はメモリ430内の乱数生成関数を使用して、メモリ430内の電話機番号と時計回路440から取得される日時データから乱数を生成しカードへ送る。因みに、時計回路440から取得される日時情報は取得の都度異なる値となるため、乱数も都度異なる値として生成される。

【0080】電話機400で生成された乱数を受け取ったカード300側では、メモリ330内の認証子生成関数を使用して、電話機で生成された乱数、メモリ330内の秘密鍵及び度数情報から認証子を生成する。生成された認証子は、メモリ330内の度数情報とともに電話機400へ送られる。

20 【0081】ICカード300からの度数情報及び認証子を受け取った電話機400は、これら度数情報及び認証子を、先に生成しICカード300へ送った乱数とともに交換機500へ送る。

【0082】この交換機500は、電話局や交換センター等に設置される、回線交換設備又は施設といったイメージのものである。交換機500は、メモリ530内の認証子生成関数と秘密鍵を使用して、電話機400から送られた度数情報及び乱数から交換機独自に認証子を生成する。さらに、交換機500は、比較部540において交換機500自身で生成された認証子と、電話機400経由で送られてきた認証子とを比較する。そして、通話可否判定部550において、比較結果から電話機400に差し込まれたICカードによる通話の可否判定が下される。例えば、自身で生成された認証子と電話機400経由で送られてきた認証子とが一致すれば、電話機400に差し込まれたICカードによる通話が許可され、回線が接続される。

40 【0083】続いて、図15を参照して第2の実施形態について説明する。図15は、この発明の第2の実施形態に係るICカード処理システムを示す図である。

【0084】この第2の実施形態では、第1の実施形態で説明したセキュリティをより強固なものとするため、認証子生成の種として全てのICカード300に対して異なる値をとるカード個別番号(各ICカードに固有の番号)を利用する。このカード個別番号は、発行機200による発行処理の際にICカード300に対して付与されるものであり、ICカード300のメモリ330に



記憶される。

【0085】すなわちICカードの製造または発行時に、全てのICカードに対して全て異なる値をとるカード個別番号を設定し、ICカード300内及び交換機500での認証子生成に利用する。そのためには、電話機400に差し込まれたICカード300のカード個別番号を交換機500へ送る必要がある。カード個別番号は、前記説明した第1の実施形態において度数情報等を交換機500へ送ると同様にして交換機500へ送られる。これによりICカードから出力され電話回線経由で伝えられる認証子をより複雑化することができる。

【0086】さらに、この第2の実施形態では、第1の実施形態で説明したセキュリティをより強固なものとするため、ICカード300と交換機500相互に同じ値を持ち合う秘密鍵を複数組用意し、必要に応じて適用する秘密鍵を変更する。これら複数組の秘密鍵は、第1の実施形態と同様に、ICカード300のメモリ320、交換機500のメモリ530に記憶される。勿論、ICカード300のメモリ320に記憶される複数組の秘密鍵と、交換機500のメモリ530に記憶される複数組の秘密鍵とは同じものである。

【0087】例えばICカード300には、発行時にK1、K2、…、Kn、…、KNの複数種の秘密鍵を格納しておき、当初はカード、交換機ともKa ( $1 \leq a \leq N$ ) で前記第1の実施形態の運用を開始する。ある一定期間を経過したりその時使用している秘密鍵が漏洩した懸念が発生した場合、ICカードが差し込まれた際に、電話機400経由で交換機500からICカード300へ、今後はKb ( $1 \leq b \leq N$ 、 $b \neq a$ ) を適用するよう設定する命令を送り、同時に交換機500側も処理にKbを適用する。この設定されたICカード300は、その後は交換機から指示がなくてもKbを処理に適用する。

【0088】また、交換機側500での秘密鍵管理はICカード300に格納されているK1～KN全てを当初から制御プログラムに包含しておき、そのいずれを適用するかを選択する方法と、常に1種類だけ保持し都度入れ替え（書き換え）る方式が考えられる。これにより、秘密鍵の解析がより困難になる。

【0089】但し、適用する鍵を変更する命令を永続的にカードに送り続けることは、システムの解析を容易にするため、鍵変更の命令を送るのは一定期間だけ（半年間程度）とし、その期間に使用されなかった（電話機400に差し込まれなかった）ICカード300については、窓口等を持ってきてもらう運用により不正カードを除去できる。

【0090】このような第2の実施形態のICカード処理システムにおけるセキュリティは次のようにして守られる。

【0091】まず、製造設備100で認証子生成関数を

含むカード制御プログラムがICカード300へ登録される。さらに、発行機200でカード個別番号、度数、及び秘密鍵1～Nがカードへ登録される。この秘密鍵は何らかの手法で予め決定されている値である。

【0092】例えば、電話機400にICカード300が差し込まれると、電話機400はメモリ430内の乱数生成関数を使用して、メモリ430内の電話機番号と時計回路440から取得される日時データから乱数を生成しカードへ送る。因みに、時計回路440から取得される日時情報は取得の都度異なる値となるため、乱数も都度異なる値として生成される。

【0093】電話機400で生成された乱数を受け取ったカード300側では、メモリ330内の認証子生成関数を使用して、電話機で生成された乱数、メモリ330内の秘密鍵とカード個別番号、及び度数情報から認証子を生成する。生成された認証子は、メモリ330内の度数情報及びカード個別番号とともに電話機400へ送られる。

【0094】ICカード300からの度数情報、カード個別番号、及び認証子を受け取った電話機400は、これら度数情報、カード個別番号、及び認証子を、先に生成しICカード300へ送った乱数とともに交換機500へ送る。

【0095】交換機500は、メモリ530内の認証子生成関数と秘密鍵を使用して、電話機400から送られた度数情報、カード個別番号、及び乱数から交換機独自に認証子を生成する。さらに、交換機500は、比較部540において交換機500自身で生成された認証子と、電話機400経由で送られてきた認証子とを比較する。そして、通話可否判定部550において、比較結果から電話機400に差し込まれたICカードによる通話の可否判定が下される。例えば、自身で生成された認証子と電話機400経由で送られてきた認証子とが一致すれば、電話機400に差し込まれたICカードによる通話が許可され、回線が接続される。

【0096】ある秘密鍵による運用が一定期間継続した場合や、秘密鍵漏洩の懸念が発生した場合、交換機500から電話機400経由で秘密鍵変更コマンドが送られ、以降運用に適用される秘密鍵が変更される。

【0097】なお、第2の実施形態で使用するカード個別番号のカードへの登録設定は、第1の実施形態を実現する各機器の中ではICカード300自体の製造時に登録してしまうか、或いは上記したように発行機200で書き込む方法が考えられる。発行機200で書き込む場合、入力編集作業として秘密鍵を設定するのと同じタイミングでの設定が考えられ、基本的に番号体系はシステムとして予め決定されていて、発行機200としてもその体系のデータを書き込む様にプログラムされているものとして、使用する（発行する）番号を指定するだけの場合や、直接キーボード等から入力する場合等がある。

【0098】続いて、図16を参照して第3の実施形態について説明する。図16は、この発明の第3の実施形態に係るICカード処理システムを示す図である。

【0099】この第3の実施形態では、第1及び第2の実施形態で説明したセキュリティをより強固なものとするため、秘密鍵をカード個別番号から生成する。

【0100】例えば、発行機200と交換機500の双方に認証子生成用秘密鍵の生成ロジックと秘密鍵生成鍵K'を設定し、この秘密鍵生成鍵K'とカード個別番号から認証子生成用秘密鍵の生成ロジックにより秘密鍵Kを生成する。すなわち、発行時にICカード300のメモリ330内に格納される秘密鍵Kは、発行機200が内蔵する秘密鍵生成ロジックによりカード個別番号と秘密鍵生成鍵K'に従い生成され、書き込まれたものとなる。また、このICカード300を使用する際、交換機500では、電話機400経由でICカード300から受け取ったカード個別番号と交換機500のメモリ530内の秘密鍵生成鍵K'から、メモリ530内の秘密鍵生成ロジックを使用して秘密鍵を生成して認証子生成に使用する。

【0101】これにより、カードに格納する秘密鍵は全てのカードで異なる値となり、システムの解析がより困難になる。

【0102】なお、この場合発行機200と交換機500双方に認証子生成用秘密鍵の生成ロジックと秘密鍵生成鍵K'を持たせる必要があるが、その方法としてそれぞれの製造段階での制御プログラムに包含しておく事が考えられる。また、このような秘密鍵Kを以下、個別秘密鍵と称する。

【0103】さらに、この第3の実施形態では、第1及び第2の実施形態で説明したセキュリティをより強固なものとするため、秘密鍵生成鍵を複数組用意し、個別秘密鍵を複数組生成し、各個別秘密鍵を対応させて使用する。

【0104】例えば、発行機200と交換機500の双方に個別秘密鍵の生成ロジックと複数の秘密鍵生成鍵K'1、K'2、…、K'n、…、K'Nを持ち、カード個別番号から複数の個別秘密鍵K1、K2、…、Kn、…、KNを生成する。

【0105】すなわち、ICカード300に格納する個別秘密鍵Knは、カード発行時にカード個別番号と秘密鍵生成鍵K'nから発行機200が内蔵する秘密鍵生成ロジックを使用して生成してカードへ書き込む。また、そのICカード300を使用する際、交換機500では電話機400経由でICカード300から受け取ったカード個別番号と交換機500のメモリ530内の秘密鍵生成鍵K'nから、メモリ530内の秘密鍵生成ロジックを使用して個別秘密鍵Knを生成して認証子生成に使用する。運用で都度使用されるnは第2の実施形態と同様に決定される。

【0106】また、交換機500側での秘密鍵管理はICカード300に格納されているK'1~K'N全てを当初から制御プログラムに包含しておき、そのいずれを適用するかを選択する方法と、常に1種類だけ保持し都度入れ替え（書き換え）る方式が考えられる。

【0107】これにより、ICカード300に格納する複数の個別秘密鍵は全てのカードで異なる値の組となり、システムの解析がより困難になる。

【0108】またさらに、この第3の実施形態では、第1及び第2の実施形態で説明したセキュリティをより強固なものとするため、各秘密鍵生成鍵ごとに異なる秘密鍵生成ロジックを適用し、単一の秘密鍵生成鍵で複数の異なる個別秘密鍵を生成する。

【0109】例えば、発行機200と交換機500の双方に複数の認証子生成用秘密鍵の生成ロジックL1、L2、…、Ln、…、LNと単一の秘密鍵生成鍵K'を持ち、カード個別番号から複数の個別秘密鍵K1、K2、…、Kn、…、KNを生成する。

【0110】すなわちICカード300に格納する個別秘密鍵Knは、カード発行時にカード個別番号と秘密鍵生成鍵K'から発行機200が内蔵する秘密鍵生成ロジックLnを使用して生成してカードへ書き込む。また、そのカードを使用する際、交換機500では電話機400経由でICカード300から受け取ったカード個別番号と交換機500のメモリ530内の秘密鍵生成鍵K'から、530内の秘密鍵生成ロジックLnを使用して個別秘密鍵Knを生成して認証子生成に使用する。運用で都度使用されるnは他の実施形態と同様に決定される。

【0111】また、交換機500側での秘密鍵管理はカードに格納されているK1~KNを生成する秘密鍵生成鍵K'と生成ロジックL1~Ln全てを当初から制御プログラムに包含しておき、いずれのLnを適用するかを選択する方法と、K'と1種類のLnだけを常に保持し都度入れ替え（書き換え）る方式が考えられる。また発行機200についても秘密鍵生成鍵K'と認証子生成用秘密鍵の複数の生成ロジックとを持つ必要があるが、その方法として製造段階での制御プログラムに包含しておく事が考えられる。

【0112】これにより、ICカード300に格納する複数の個別秘密鍵は全てのカードでより複雑な関係を持った異なる値の組となり、システムの解析がより困難になる。

【0113】さらにまた、この第3の実施形態では、第1及び第2の実施形態で説明したセキュリティをより強固なものとするため、異なる秘密鍵生成鍵ごとに異なる秘密鍵生成ロジックを適用し異なる個別秘密鍵を生成する。

【0114】例えば、発行機200と交換機500の双方に複数の認証子生成用秘密鍵の生成ロジックL1、L2、…、Ln、…、LNと各Lnに対応する秘密鍵生成

鍵 $K'n$ を持ち、カード個別番号から複数の個別秘密鍵を生成する。

【0115】すなわちカードに格納する個別秘密鍵 $K'n$ は、カード発行時にカード個別番号と秘密鍵生成鍵 $K'n$ から発行機200が内蔵する秘密鍵生成ロジック $L'n$ を使用して生成してICカード300へ書き込む。また、そのICカード300を使用する際、交換機500では電話機400経由でICカード300から受け取ったカード個別番号と交換機500のメモリ530内の秘密鍵生成鍵 $K'n$ から、メモリ530内の秘密鍵生成ロジック $L'n$ を使用して個別秘密鍵 $K'n$ を生成して認証子生成に使用する。運用で都度使用される $n$ は他の実施形態と同様に決定される。

【0116】また、交換機500側での秘密鍵管理はICカード300に格納されている $K1 \sim KN$ を生成する秘密鍵生成鍵 $K'n$ と生成ロジック $L1 \sim Ln$ 全てを当初から制御プログラムに包含しておき、いずれの $L'n$ を適用するかを選択する方法と、1種類の $K'n$ と1種類の $L'n$ だけを常に保持し都度入れ替え（書き換え）る方式が考えられる。また発行機200についても複数の秘密鍵生成鍵 $K'n$ と認証子生成用秘密鍵の複数の生成ロジック $L'n$ を持つ必要があるが、その方法として製造段階での制御プログラムに包含させておく事が考えられる。

【0117】これにより、ICカード300カードに格納する複数の個別秘密鍵は全てのICカード300でより複雑な関係を持った異なる値の組となり、システムの解析がより困難になる。

【0118】このような第3の実施形態のICカード処理システムにおけるセキュリティは次のようにして守られる。

【0119】まず、製造設備100で認証子生成関数を含むカード制御プログラムがICカード300へ登録される。さらに、発行機200でカード個別番号、度数、及び複数の個別秘密鍵 $1 \sim N$ がカードへ登録される。個別秘密鍵 $1 \sim N$ は、発行機200のメモリ230内のカード個別番号と複数の秘密鍵生成鍵 $1 \sim N$ を基にして対応する複数の秘密鍵生成関数 $1 \sim N$ により生成されたものである。

【0120】例えば、電話機400にICカード300が差し込まれると、電話機400はメモリ430内の乱数生成関数を使用して、メモリ430内の電話機番号と時計回路440から取得される日時データから乱数を生成しカードへ送る。因みに、時計回路440から取得される日時情報は取得の都度異なる値となるため、乱数も都度異なる値として生成される。

【0121】電話機400で生成された乱数を受け取ったカード300側では、メモリ330内の認証子生成関数を使用して、電話機で生成された乱数、メモリ330内の個別秘密鍵 $n$ 及び度数情報から認証子を生成する。

生成された認証子は、メモリ330内の度数情報及びカード個別番号とともに電話機400へ送られる。

【0122】ICカード300からの度数情報、カード個別番号、及び認証子を受け取った電話機400は、これら度数情報、カード個別番号、及び認証子を、先に生成しICカード300へ送った乱数とともに交換機500へ送る。

【0123】交換機500は、メモリ530内の秘密鍵生成関数 $n$ と秘密鍵生成鍵 $n$ を使用して、電話機400に差し込まれたカードに対応する個別秘密鍵 $n$ を生成する。そして、この生成された個別秘密鍵 $n$ とメモリ530内の認証子生成関数により、電話機400から受け取られた度数情報及び電話機400が生成した乱数から交換機独自に認証子を生成する。さらに、交換機500は、比較部540において交換機500自身で生成された認証子と、電話機400経由で送られてきた認証子とを比較する。そして、通話可否判定部550において、比較結果から電話機400に差し込まれたICカードによる通話の可否判定が下される。例えば、自身で生成された認証子と電話機400経由で送られてきた認証子とが一致すれば、電話機400に差し込まれたICカードによる通話が許可され、回線が接続される。

【0124】ある個別秘密鍵による運用が一定期間継続した場合や、個別秘密鍵漏洩の懸念が発生した場合、交換機500から電話機400経由で個別秘密鍵変更コマンドが送られ、以降運用に適用される個別秘密鍵が変更される。個別秘密鍵が変更されるということは、秘密鍵生成鍵及び秘密鍵生成関数が変更されるということである。

【0125】最後に、図17～図22を参照して、上記説明した機器による運用の際のICカード300～電話機400～交換機500の間で交換される通信電文の形式と内容について説明する。

【0126】これらの電文は電話機400が独自にICカード300とやりとりする場合と、電話機400が交換機500とICカード300のやりとりを仲介するだけの場合がある。

【0127】ICカード300は通常外部からの命令に従って動作する。つまり外部からの命令電文を受け取り、それに応える形で応答電文を返す動作が基本となる。図17は、それら命令電文と応答電文双方に共通な電文の全体形式を示している。電文全体としてはその命令、応答の内容を示す本体部を伝送制御情報が挟む形となる。

【0128】図18～図22は、この命令、応答の内容を示す本体部の形式内容についてのものである。

【0129】基本的に本体部は命令電文については命令内容をコード情報として始めに示し、以降その命令実行に必要な情報が付加される。また、応答電文は指示された命令内容の実行結果を示すコード情報を始めに示し、

以降その命令の実行結果として伝える必要のある情報が付加される。

【0130】図18はキー照合電文の本体部を示しており、前記の例では発行機200の設定用カードから秘密鍵を読み出す際の照合用キーの照合に使用する。

【0131】図19はデータ書き込み電文の本体部であり、前記の例では発行機200でICカード300を発行する際のICカード300への各種データ書き込みに使用する。

【0132】図20はデータ書き込み電文の本体部を示しており、前記の例では運用の中で電話機400がICカード300から各種データを読み出す際に使用する。

【0133】図21は認証子生成電文の本体部を示しており、前記の例では運用の中で電話機400がICカード300に対して乱数を渡して認証子を生成させる際に使用する。

【0134】図22は秘密鍵変更電文の本体部を示しており、運用に適用する秘密鍵を変更する際にICカード300に対して今後どのキーを適用するかを指示して変更させる際に使用する。

【0135】

【発明の効果】この発明によれば、セキュリティの要となる秘密情報（秘密鍵等）が漏洩しにくく、また、このような秘密情報が漏洩した場合でも、漏洩した秘密情報による不正使用を防止できるICカード処理システムを提供することができる。

【図面の簡単な説明】

【図1】ICカードの外観を示す図。

【図2】ICカードの製造手順を示すフローチャート。

【図3】ICチップの概略構成を示す図。

【図4】発行機の外観を示す図。

【図5】発行機によるICカードの発行を説明するフローチャート。

【図6】設定用ICカードを説明するための図。

【図7】設定用ICカードを説明するための図。

【図8】設定用ICカードを説明するための図。

【図9】相互認証を説明するための図。

【図10】電話機の外観を示す図。

【図11】電話機の製造手順を示すフローチャート。

【図12】交換機の外観を示す図。

【図13】交換機の製造手順を示すフローチャート。

【図14】この発明の第1の実施形態に係るICカード処理システムを示す図。

【図15】この発明の第2の実施形態に係るICカード処理システムを示す図。

【図16】この発明の第3の実施形態に係るICカード処理システムを示す図。

【図17】ICカードの電文の全体形式の概略を示す図。

【図18】キー照合電文の本体部の概略を示す図。

【図19】データ書き込み電文の本体部の概略を示す図。

【図20】データ読み出し電文の本体部の概略を示す図。

【図21】認証子生成電文の本体部の概略を示す図。

【図22】適用秘密鍵変更電文の本体部の概略を示す図。

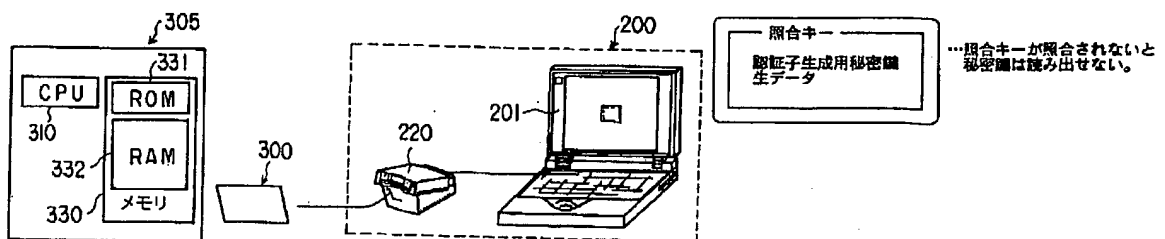
【符号の説明】

- 200…発行機
- 210…発行機CPU
- 220…カードリーダー・ライタ
- 230…メモリ
- 300…ICカード
- 310…ICカードCPU
- 320…インターフェイス
- 330…メモリ
- 400…電話機
- 410…電話機CPU
- 420…インターフェイス
- 430…メモリ
- 440…時計回路
- 500…交換機
- 510…交換機CPU
- 520…インターフェイス
- 530…メモリ
- 540…比較部
- 550…通話可否判定部

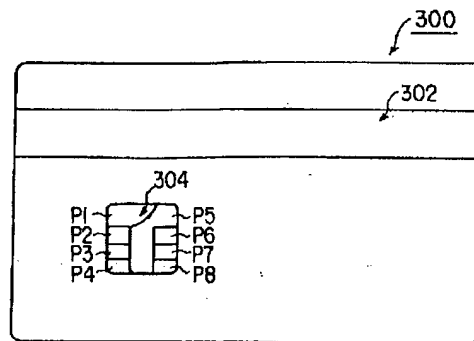
【図3】

【図4】

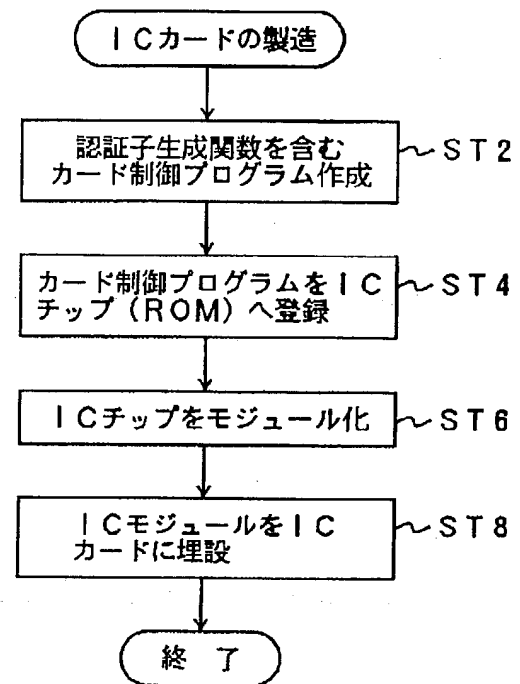
【図6】



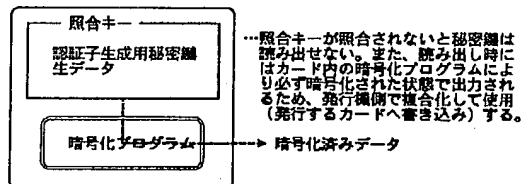
【図1】



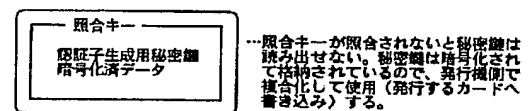
【図2】



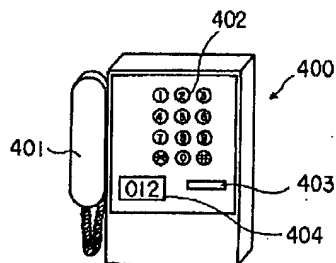
【図7】



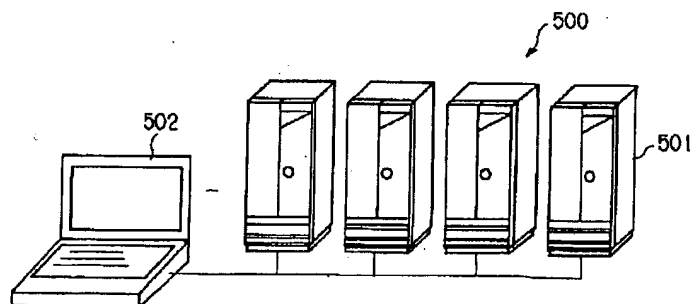
【図8】



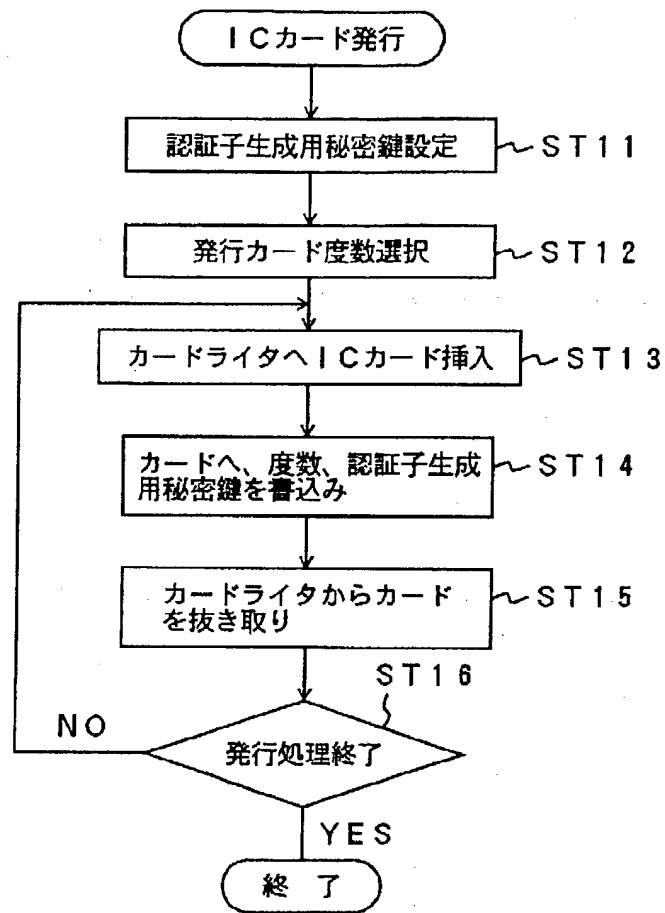
【図10】



【図12】



【図5】



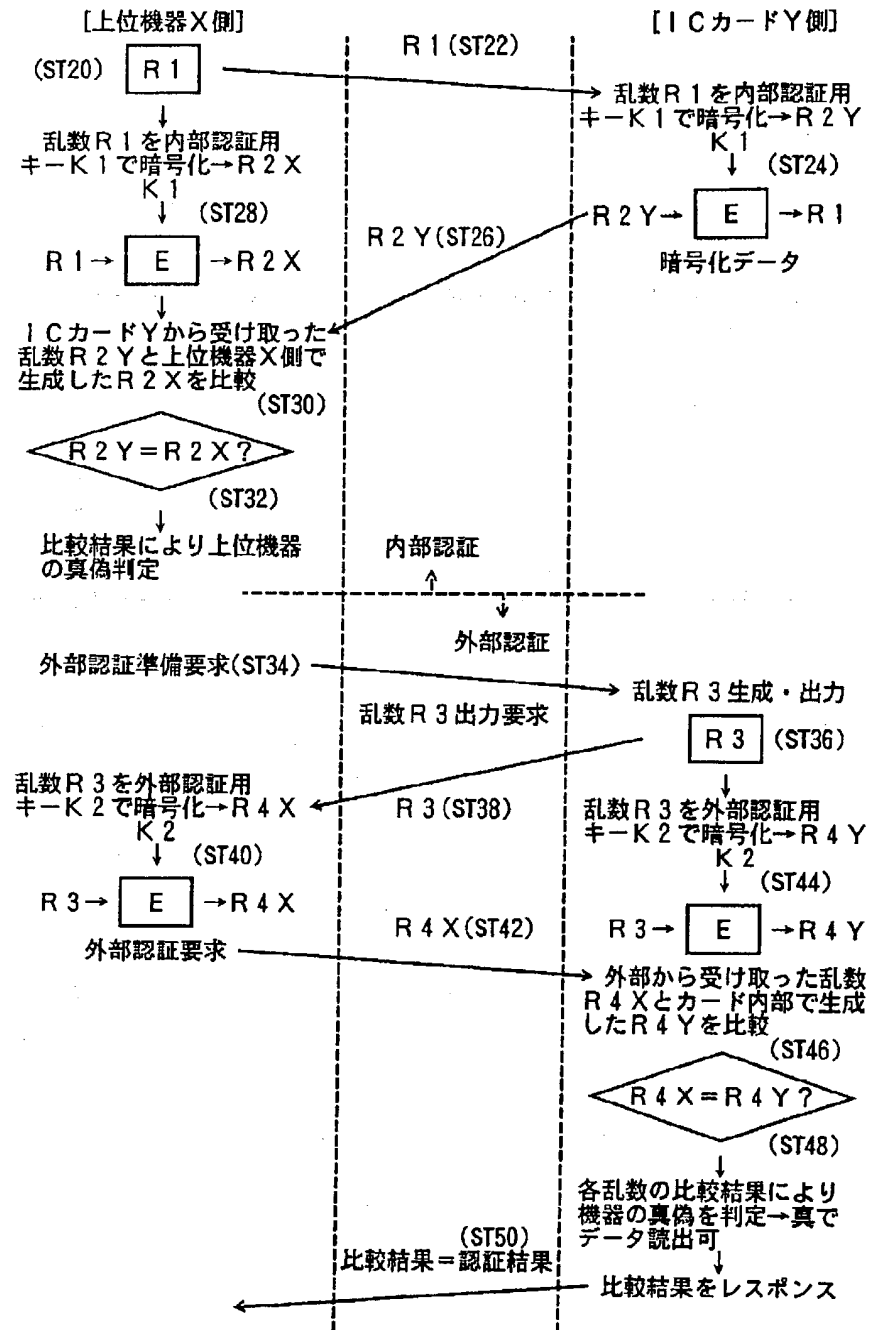
【図17】

送信元 識別符号	送信先 識別符号	本体部 データ長	[本体部]	誤り 検出信号
-------------	-------------	-------------	-------	------------

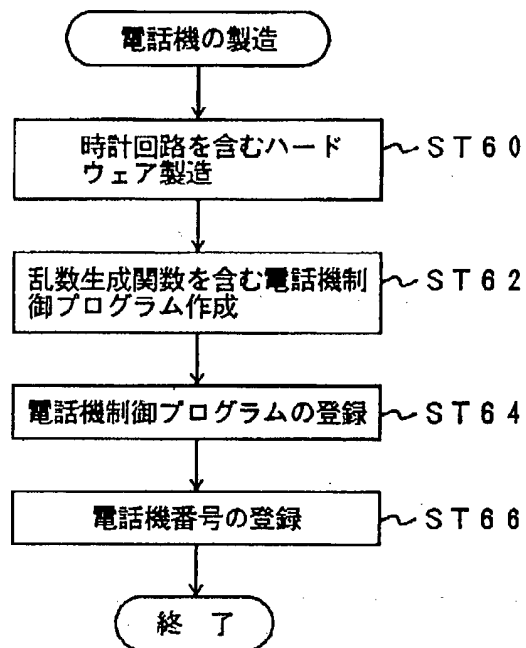
【図18】

命令電文:	キー照合命令コード	照合対象キー識別子	照合キー値
応答電文:	照合結果表示コード		

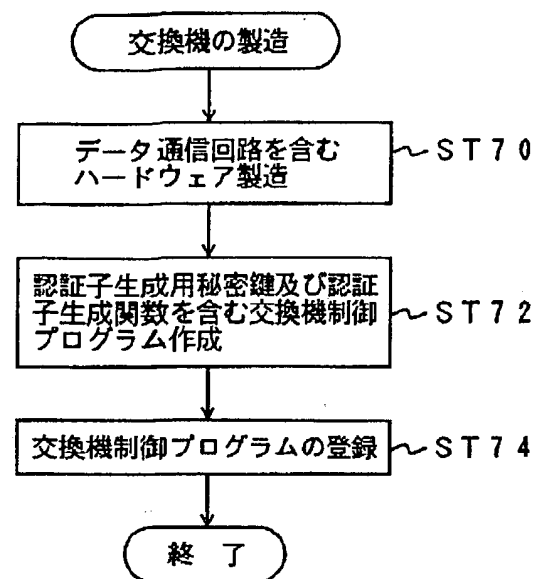
【図9】



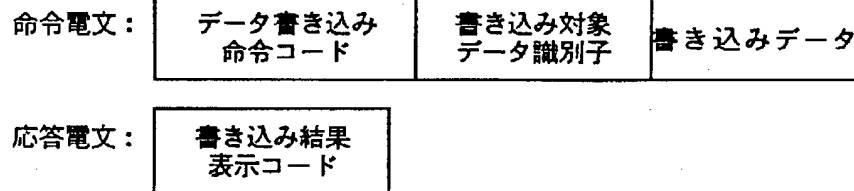
【図11】



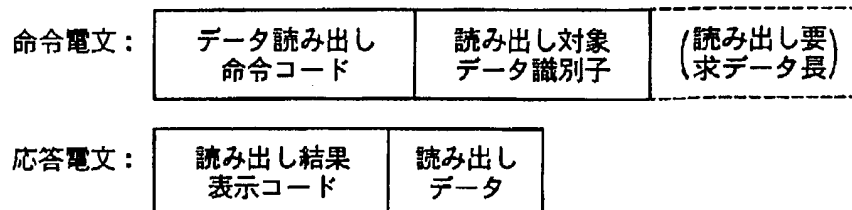
【図13】



【図19】

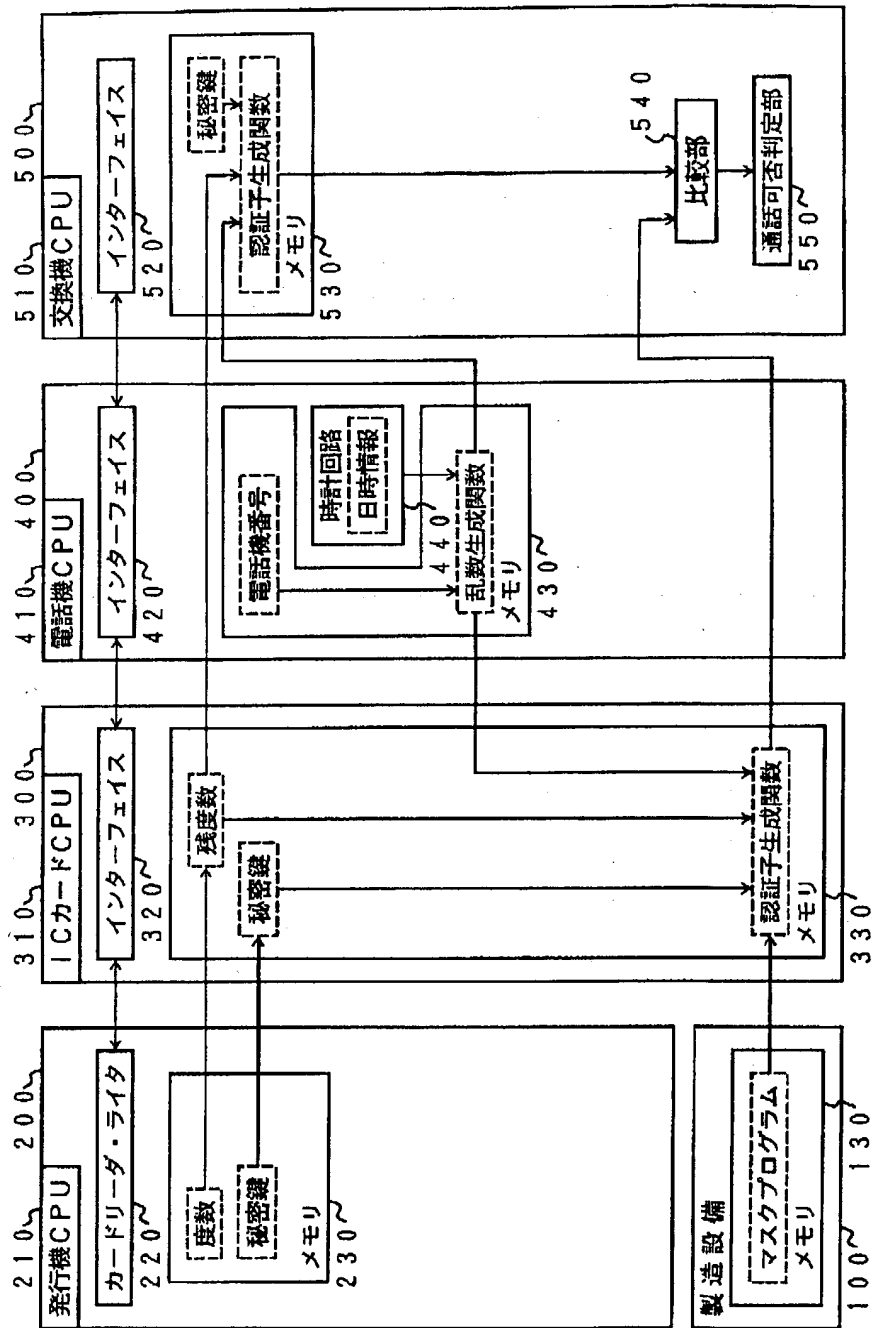


【図20】

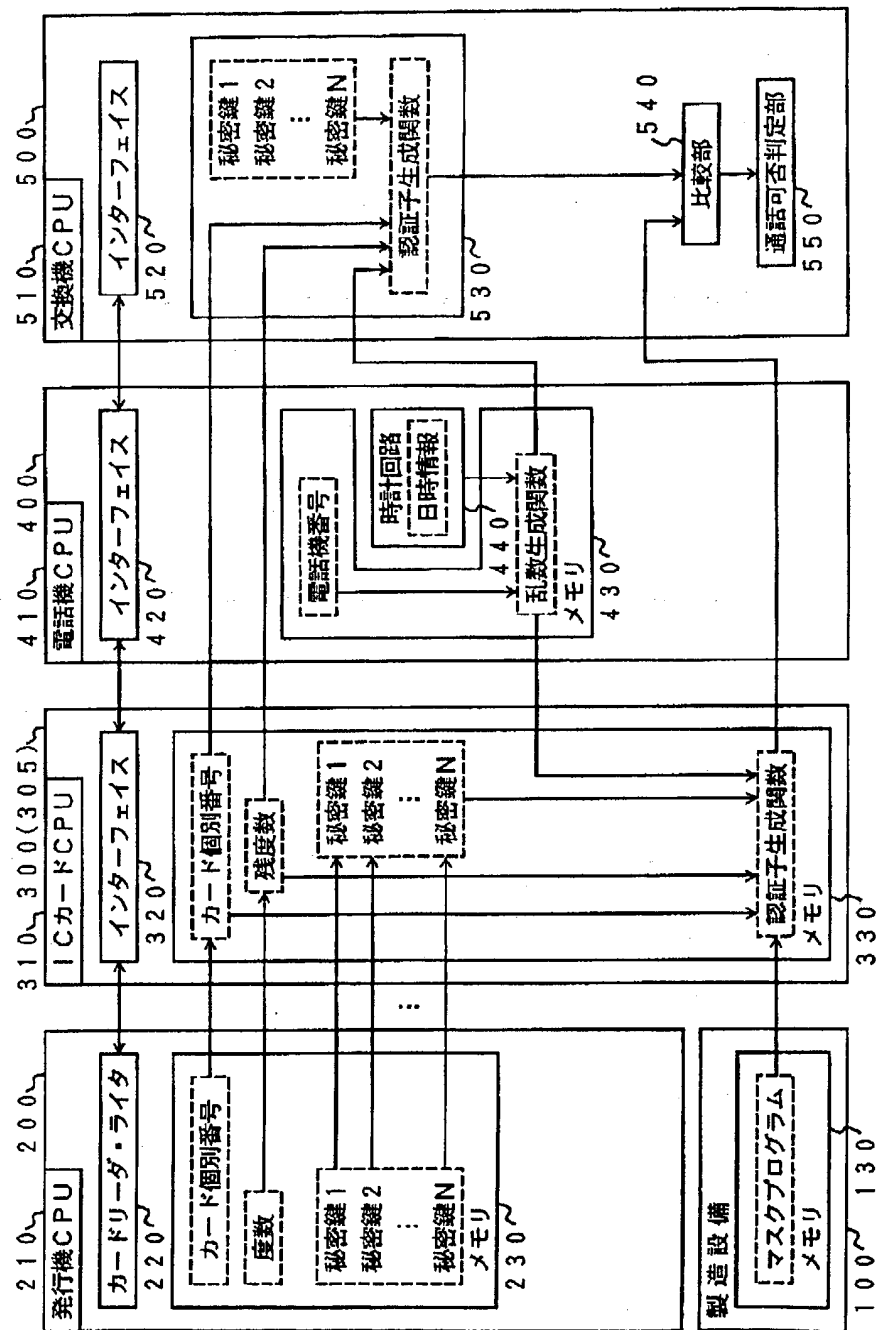




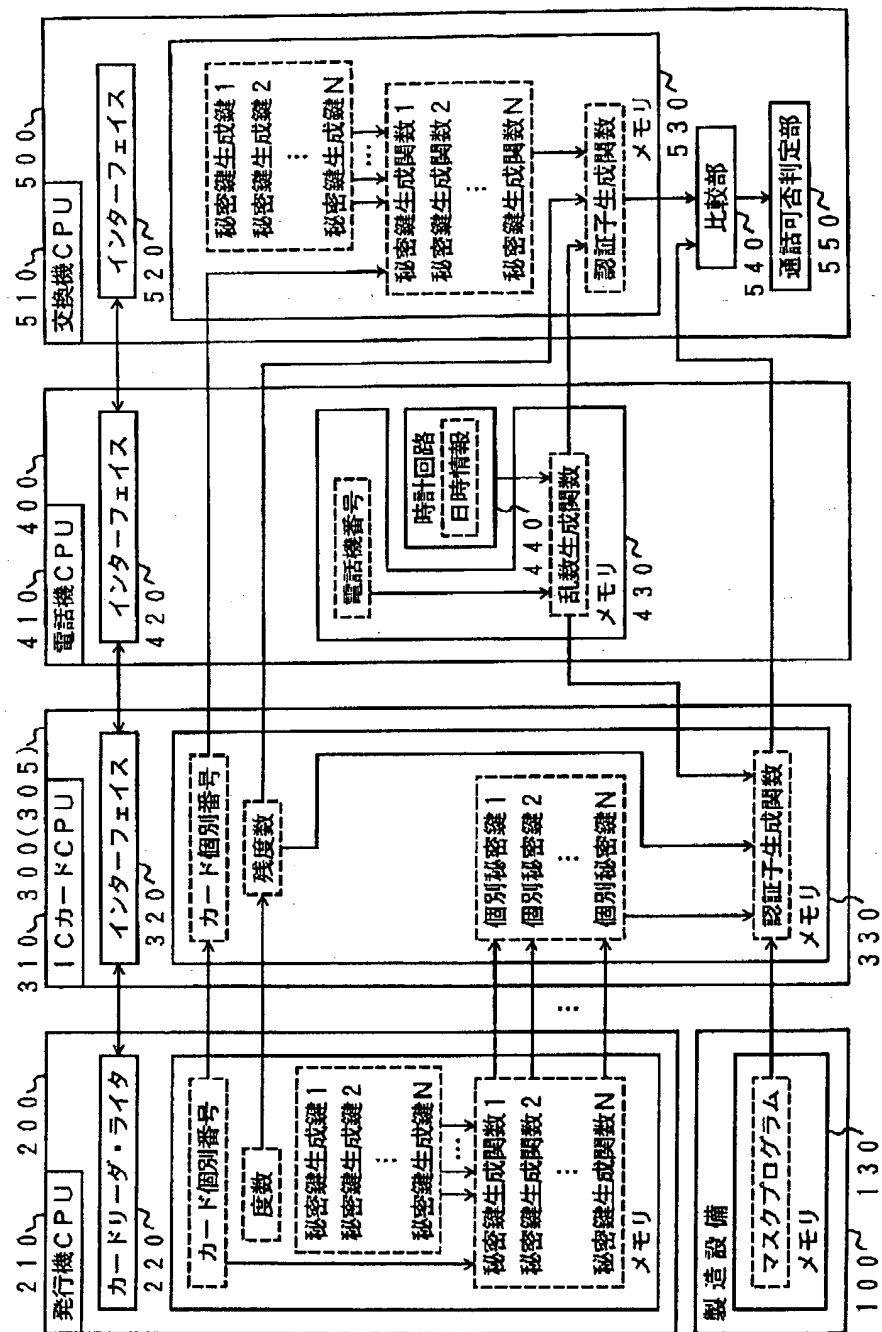
【図14】



【図15】



【図16】



【図21】

命令電文： 

認証子生成命令コード	乱数
------------	----

応答電文： 

認証子生成結果表示コード	認証子データ
--------------	--------

【図22】

命令電文： 

適用秘密鍵変更命令コード	変更後値
--------------	------

応答電文： 

適用秘密鍵変更結果表示コード
----------------

---

フロントページの続き

(51) Int. Cl.<sup>6</sup>

H 0 4 M 15/00  
17/02

識別記号

F I

G 0 6 K 19/00

R  
U